Research Paper | Computer Sci. | E-ISSN No : 2454-9916 | Volume : 11 | Issue : 5 | May 2025

REVIEW OF AUTHENTICATION AND SECURITY FRAMEWORKS FOR THE INTERNET OF THINGS (IoT)

Vaidehi Shah[1], Dr. Vijaykumar B Gadhavi[2]

[1] Research Scholar, Computer Engineering Department Swaminarayan University, India
[2] Associate Professor & Dean –Faculty of Engineering, Computer Engineering Department, Swaminarayan University, India

ABSTRACT

The Internet of Things (IoT) is transforming the modern digital landscape by enabling seamless connectivity among billions of devices. However, the rapid growth of IoT networks has introduced critical security challenges, particularly in authentication, due to the heterogeneous, distributed, and resource-constrained nature of IoT environments. This review explores the evolving landscape of authentication mechanisms in IoT, highlighting their significance in mitigating common threats such as impersonation, replay, and man-in-the-middle attacks. The paper presents a comparative study of existing authentication approaches, including identity-based, token-based, PUF-based, and context-aware methods, assessing them on parameters like security robustness, computational overhead, and hardware compatibility. Through a comprehensive literature review, we identify current limitations in traditional models and propose potential enhancements aimed at developing lightweight, scalable, and energy-efficient authentication frameworks. This study contributes to the ongoing discourse on IoT security by outlining future research directions to achieve secure, reliable, and context-aware authentication mechanisms suitable for the dynamic IoT ecosystem.

KEYWORDS: IoT Vulnerabilities, Security Frameworks, Future Directions in IoT

1. INTRODUCTION

1.1 Overview of IoT and Its Growth

The Internet of Things (IoT) encompasses a vast network of interconnected physical devices—referred to as "things"—equipped with sensors, software, and communication technologies that enable them to collect and exchange data over the internet. These devices span diverse domains, from consumer-level applications such as smart home systems and wearable health monitors to mission-critical deployments in manufacturing, healthcare, and transportation. IoT has emerged as a key driver of innovation in areas like smart agriculture, urban infrastructure, and supply chain management [6], [7]. As industry forecasts predict that the number of IoT-connected devices will exceed 30 billion by 2030, the role of IoT in enhancing automation, operational efficiency, and real-time decision-making continues to expand rapidly.

1.2 Importance of Security and Authentication in IoT

While IoT offers substantial benefits, its decentralized and heterogeneous nature, combined with the limited processing and storage capacities of edge devices, creates significant security vulnerabilities. Among the various components of IoT security, authentication plays a critical role in verifying the identities of users and devices within the network [1], [3]. In the absence of robust authentication protocols, IoT systems are susceptible to a range of cyber threats, including unauthorized access, data breaches, impersonation attacks, and denial-of-service (DoS) attacks [2], [4], [5]. Given that traditional authentication mechanisms are often too resource-intensive for IoT devices, there is an urgent need for lightweight solutions that maintain a strong security posture without overburdening device resources [31], [32].

1.3 Motivation Behind the Survey

The increasing complexity of secure communication in the IoT landscape has led to the development of a wide range of authentication methods, from conventional password- and token-based systems to more sophisticated schemes utilizing elliptic curve cryptography (ECC), Physical Unclonable Functions (PUFs), and biometric verification [3], [31], [32]. However, these techniques exhibit substantial variation in terms of implementation complexity, computational overhead, and suitability for constrained environments. This diversity highlights the importance of a comprehensive survey that not only maps the current state of IoT authentication strategies but also identifies key challenges and areas where further innovation is required [5], [6], [8].

1.4 Scope and Objectives of the Paper

This review focuses on evaluating contemporary and emerging authentication protocols tailored for IoT environments. It aims to systematically analyze their performance, scalability, and resilience against evolving security threats. The specific objectives of this study are:

- To categorize and critically assess lightweight authentication mechanisms used in IoT systems [1], [31], [32].
- To analyze trade-offs between core performance indicators, including security robustness, computational efficiency, and energy consumption [6], [11].
- To identify authentication approaches with the highest potential for real-world IoT deployment.
- To provide informed perspectives and research directions that can advance the future of secure IoT infrastructures [5], [8].

1.5 Contribution Summary

This paper offers several key contributions:

- A comprehensive review of 18 influential research publications addressing authentication and security issues in IoT from 2017 to 2025 [1]–[32].
- A comparative analysis of various authentication techniques, such as cryptographic (ECC, AES), biometric, password/token-based, and hybrid approaches [3], [10], [11], [31].
- An identification of the limitations inherent in existing solutions, including scalability issues, high energy consumption, and exposure to side-channel and physical attacks [31], [32].
- A discussion on ongoing challenges and emerging trends in the field, including AI-driven anomaly detection, context-aware authentication strategies, and privacy-enhancing technologies [5], [6], [7], [13].

2. LITERARURE REVIEW

	Title	Authors	Publication	Fundamental Thought	Recommend Improvement
1	A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs[31]	I. Cetintav and M. Tahir Sandikkaya	IEEE Access, 2025	• Importance of authentication service in IoT • Considered Authentication Factors- Password, RFID, OTP & Smart Card. • Frequently Used Cryptographic Primitives- ECC, PUF. • Idea about the different Parameters- Communication Cost, Computational Cost for validating effectiveness of Authentication Approach.	PUF based approach will require more resources for computing Challenge- Response. • - ECC based approch will be complex in Implementation, will require higher computational resources to generate a pair of key and also vulnerable to Side Channel Attacks
2	Network Efficient Hierarchical Authentication Algorithm for Secure Communication in IoT and IoE[32]	A. Sharma, R. Suganya, P. B. Krishna, R. Raj and R. Kumar Murugesan	IEEE Access, 2024	• A Novel Encryption Method – Network Efficient Hierarchical Authentication is presented. • AES Encryption Method is used in NOVA Method. • Dynamic Key is generated for AES Encryption by using MAC Address of Device. • NEHA uses a 140-bit data transfer scheme, surpassing the traditional 128-bit standard, significantly boosting resistance to direct attacks.	AES algorithms are resource-intensive, • -IoT devices, especially those with limited resources, struggle to execute these operations efficiently and quickly, potentially leading to delays and increased energy consumption, which can shorten battery life
3	Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios	Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L	Journal of Electronics, MDPI, 2023	• Different Methods for IoT Authentication- Password Based, Token Based, Biometric Authentication & Cryptographic Authentication.	• -Efficient and Secure Authentication Method can be developed by considering multiple factors for enhancing security.
4	Security and Internet of Things: Benefits, Challenges, and Future Perspectives[1]	Hamed Taherdoost et al.	MDPI, 2023	• Discussed IoT security requirements. • Highlighted the importance of authentication and current IoT security issues.	Authentication, Data Security, Network Security, Current Security Challenges

5	A Review on Security in Internet of Things[2]	Eisha Akansha, Abhishek Javali et al.	IEEE, 2022	• Discussed security attacks on IoT at different layers. • Suggested security measures to mitigate these threats.	Layer-wise Security Attacks, Mitigation Strategies, Security Measures
6	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures[3]	Vikas Hassija, Vinay Chamola	IEEE, 2019	• Compared traditional security with IoT security. • Highlighted the absence of standards, system limitations, and open architecture as key challenges.	Security Threats, Traditional vs. IoT Security, Solution Architectures, Open Architecture
7	Study of Security Issues and Solutions in Internet of Things (IoT)[4]	Shashi Rekha, Lingala Thirupathi et al.	Elsevier, 2021	• Discussed the importance of security in IoT. • Identified approaches to address security challenges in IoT networks.	Security Challenges, Approaches for IoT Security, Physical, Information, and Operational Security
8	Insight to Security Paradigm, Research Trend & Statistics in Internet of Things (IoT)[5]	Jyoti Neeli, Shamshekhar Patil et al.	Elsevier, 2021	• Identified privacy and security challenges. • Highlighted open research issues and reviewed recent work on authentication, intrusion detection, and data protection.	Privacy, Security Paradigm, Open Research Issues, Authentication, Intrusion Detection
9	Security trends in Internet of Things: a survey[6]	Rachit, Shobha Bhatt & Prakash Rao Ragiri	Springer Nature 2021	The Internet of Things (IoT) is a network of uniquely identifiable embedded devices that communicate via transient states. This study examines security challenges related to current IoT standards and protocols, reviewing risks, novel security protocols, and recent projects. It emphasizes the need for standardization in communication and data auditing to address system vulnerabilities. Additionally, the research underscores the importance of developing protocols that can counter multiple threat vectors as IoT expands from small networks to wide area environments, increasing security risks.	A clearer focus on specific case studies of IoT security breaches in different sectors (e.g., healthcare, industrial IoT, etc.) could be included. Recommendations for specific standards and practical strategies for mitigating emerging security risks in larger IoT environments could be more elaborated.
10	The 10 Research Topics in the Internet of Things[7]	Wei Emma Zhang, Quan Z. Sheng et al.	IEEE, 2020	• Identified ten key research domains in IoT. • Emphasized energy harvesting, data-driven IoT, and security and privacy as critical areas	Energy Harvesting, Data-Driven IoT, IoT Search, Security & Privacy, Edge Computing
11	Internet of Things: Future Challenging Issues and Possible Research Directions[8]	Amit Kumar Tyagi, Ajith Abraham	IEEE, 2020	• Discussed potential research issues and challenges in IoT. • Highlighted problems such as heterogeneity, context awareness, middleware, and security.	Heterogeneity, Context Awareness, Middleware, Energy Management, Security
12	IoT Security Issues[9]	Hyungsik Shin, Ho Kyoung Lee	IEEE, 2019	• Explained the CIA model of security and its relevance to IoT. • Identified security challenges across IoT layers (Perception, Network, Application).	CIA Model, Security Challenges by IoT Layer, Threats (e.g., Node Capture, Spoofing, DDoS)
13	Security in Internet of Things: Issues, Challenges, and Solutions[10]	Hanan Aldowah, Irfan Kumar et al	Springer Nature, 2019	• Identified security issues and proposed solutions in IoT. • Discussed strategies for securing IoT networks and devices.	Security Issues, Solution Strategies, IoT Networks, Device Security
14	Multi-stage security model using ECC and FHE[11]	Priyanka et al	Springer 2019	Ensures data integrity with less computational power, but has issues with increased data overheads and computational cost	Cryptographic Attacks, Data Integrity

15	Low-scale Denial-of-Service attack detection in Zigbee WSN using Trust evaluation and Hilbert-Huang[12]	Chen, Hongsong	IEEE,2019	Scalable architecture, useful in cloud and edge computing IoT devices, but larger storage overheads remain an issue	DoS Attack Detection, Low Energy Devices
16	Analysis of Security and Privacy Challenges in Internet of Things[13]	Jean Pierre Nzabahi-mana	IEEE, 2018	• Examined security and privacy challenges in IoT. • Discussed potential research directions for enhancing IoT security.	Security & Privacy Challenges, Research Directions, Privacy Preservation
17	A Closer Look at the IoT's Things[14]	Jeffry Voas, Bill Agersti	IT Professional, 2018	• Provided insights into the components of IoT. • Discussed the importance of securing "things" within the IoT ecosystem.	IoT Components, Device Security, Network Security
18	A Systematic Study of Security Issues in Internet-of-Things (IoT)[15]	B. V. S. Krishna, T. Gnanasekaran	IEEE, 2017	• Systematic review of IoT security challenges. • Identified potential threats and proposed security solutions.	Security Challenges, Systematic Review, Threats, Security Solutions

3. SECURITY ISSUES

The rapid expansion of the Internet of Things (IoT) has introduced a diverse set of security concerns that must be addressed to ensure safe, reliable, and privacy-preserving environments. Based on the reviewed literature, the following critical security issues in IoT ecosystems are identified:

Figure 1. Types of Attacks

A. Multi-Layer Security Threats

IoT architectures are generally divided into three layers—Perception, Network, and Application. Each layer is vulnerable to unique security threats. The Perception Layer is susceptible to physical attacks such as node capture and side-channel attacks. The Network Layer faces risks like Sybil attacks, routing disruption, and Denial-of-Service (DoS) attacks. The Application Layer is prone to data breaches, unauthorized access, and malware injection [9], [12].

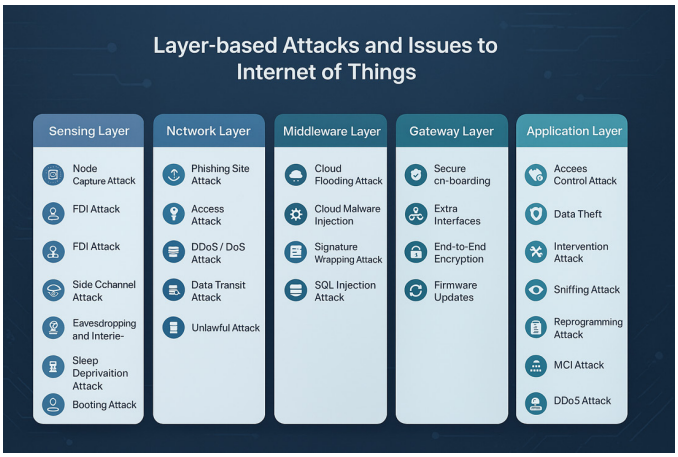

Figure 2. Layer Based Attacks and Issues to Iot - Adapted From [3]

B. Absence of Standardized Protocols

A lack of global security standards for IoT results in non-uniform security implementations. Open and heterogeneous architectures complicate enforcement, making devices vulnerable to various attacks due to inconsistencies in protocol and encryption practices [3], [6].

C. Authentication Constraints

IoT devices often operate under strict resource constraints, making traditional authentication mechanisms inefficient. Researchers have proposed lightweight authentication protocols using ECC, PUFs, and MAC-based encryption schemes. While these approaches reduce overhead, they present challenges related to implementation complexity, energy consumption, and susceptibility to side-channel attacks [31], [32].

D. Privacy Risks

IoT systems continually collect and transmit vast amounts of personal and sensitive data, leading to significant privacy concerns. Improper data handling and weak access controls can result in unauthorized data exposure or profiling, particularly in healthcare and smart home applications [5], [13], [16].

E. Computational and Cryptographic Limitations
Although cryptographic techniques like AES and ECC are widely adopted, their high computational demands are unsuitable for constrained IoT devices. This leads to trade-offs between security and performance, often compromising either processing speed or energy efficiency [11], [32].

F. Denial-of-Service (DoS) and Distributed DoS Attacks
Due to their always-connected nature, IoT systems are frequently targeted by DoS and DDoS attacks. While lightweight detection models using trust evaluation and signal analysis techniques such as the Hilbert-Huang Transform have been proposed, practical implementations are still evolving [12].

G. Device and Firmware Vulnerabilities
Unsecured firmware and outdated software in IoT devices offer exploitable entry points. Measures such as secure boot, signed firmware updates, and tamper-resistant design are critical but often lacking in commercial devices [14], [17].

H. Data Integrity and Trust
Ensuring data authenticity and integrity is essential, especially in mission-critical IoT systems. Multi-stage encryption models and trust-based data validation have shown promise, yet they can lead to increased communication overheads and are not yet optimized for large-scale deployment [11], [8].

I. Intrusion Detection Deficiencies
Resource limitations hinder the deployment of real-time intrusion detection systems (IDS) in IoT environments. Recent studies focus on adaptive, low-power IDS solutions tailored to edge and fog computing, though standardization is still needed [5], [13].

J. Emerging Threat Surfaces
With IoT adoption expanding into sectors like industrial automation, autonomous vehicles, and smart cities, new threat vectors continue to emerge. This requires the development of dynamic, cross-domain, and context-aware security architectures [6], [10], [13].

4. CURRENT SECURITY MECHANISM FOR IoT

Security Approach	Core Features	Application Focus	References from Survey
Blockchain-Based	Decentralized, immutable data ledger, enhanced transparency, smart contract usage	Secure data sharing, authentication, integrity	[1], [5], [10]
Fog Computing	Edge-level processing, reduced latency, data filtering near source	Real-time processing in healthcare, smart cities	[6], [11], [12]
Machine Learning (ML)	Anomaly detection, intrusion prevention, predictive threat analysis	Security monitoring, intrusion detection	[5], [8], [13]
Edge Computing	Local data processing, bandwidth optimization, device-level security	Industrial IoT, smart homes	[2], [7], [15]
Cryptographic Methods	Data confidentiality, secure transmission, key management	All layers: sensing to application	[3], [4], [11], [14]
Access Control Models	Authentication, authorization, identity verification	User/device level security in smart environments	[1], [3], [9], [13]

TABLE 1: Classification of Various Security Areas for IoT With Respect to Applications

5. FUTURE DIRECTIONS IN IoT SECURITY

As the Internet of Things (IoT) continues to expand across various sectors, ensuring robust security across all layers—device, network, and application—has become increasingly critical. With growing complexity and emerging threats, future research must focus on the development of adaptive, lightweight, and scalable security solutions. The following directions highlight key areas for further exploration:

1. Integrated Security Across IoT Layers
A unified security approach that spans all layers of the IoT architecture is essential. Future work should focus on designing comprehensive frameworks that address vulnerabilities at the device, network, and application levels, ensuring consistent and end-to-end protection across heterogeneous IoT environments (Shin & Lee, 2019) [9].

2. Lightweight Cryptography and Authentication
Due to limited computational and energy resources, many IoT devices struggle with traditional cryptographic methods. Researchers are encouraged to develop lightweight and efficient algorithms—such as Elliptic Curve Cryptography (ECC) and Physically Unclonable Functions (PUF)—that offer strong security while maintaining operational feasibility for constrained devices (Cetintav & Sandikkaya, 2025) [31].

3. Privacy Protection
The pervasive collection of personal and sensitive data in IoT applications necessitates stronger privacy measures. Future research should prioritize privacy-preserving techniques, including Fully Homomorphic Encryption (FHE), differential privacy, and secure multi-party computation, particularly in domains like healthcare and smart environments (Neeli et al., 2021) [5].

4. Artificial Intelligence and Machine Learning for Security

AI and ML hold promise for dynamic threat detection and real-time anomaly recognition. Adaptive models can strengthen intrusion detection systems (IDS) and enhance network defense. However, future research must also address the susceptibility of these models to adversarial attacks to ensure their reliability and resilience (Nzabahimana, 2018) [13].

5. Blockchain for Decentralized Security

Blockchain technology offers decentralized, tamper-resistant data management, which can enhance authentication, integrity, and traceability in IoT networks. Nevertheless, limitations such as scalability, energy overhead, and latency must be resolved to enable broader adoption in real-time and large-scale IoT systems (Hassija & Chamola, 2019) [3].

6. Edge and Fog Computing for Enhanced Security

Shifting security functions to the edge of the network reduces response time and minimizes exposure to central vulnerabilities. Edge and fog computing models allow for local threat detection and data filtering. Future research should focus on developing efficient edge-based IDS and encryption techniques to support latency-sensitive applications (Sharma et al., 2024) [32].

7. Developing IoT Security Standards

The lack of uniform standards across IoT platforms creates security gaps and interoperability issues. There is a pressing need for globally accepted frameworks and protocols that define baseline requirements for authentication, encryption, device communication, and firmware updates (Akansha et al., 2022) [2].

8. Energy-Efficient Security Solutions

Energy consumption remains a key constraint in IoT security, especially for battery-operated and remote devices. Research should explore power-aware encryption methods, adaptive security levels, and mechanisms such as duty cycling and lightweight cryptography to reduce energy impact while maintaining security effectiveness (Rekha et al., 2021) [4].

9. Hybrid Blockchain and AI-Based Security Models

The integration of blockchain with AI can result in more secure and intelligent IoT systems. Blockchain ensures data integrity and transparency, while AI can detect anomalies and predict threats based on transaction patterns. This synergy could be pivotal for automated and scalable security frameworks (Taherdoost et al., 2023) [1].

10. Security in Industrial IoT (IIoT)

As industrial systems integrate IoT for automation and monitoring, they become targets for high-impact attacks. Securing Industrial IoT (IIoT) systems demands real-time surveillance, robust intrusion detection, and secure update mechanisms to protect mission-critical operations such as SCADA and PLC-based systems (Aldowah et al., 2019) [10].

6. CONCLUSION

The Internet of Things (IoT) is transforming industries such as healthcare and manufacturing by linking embedded devices that exchange and process data. However, as IoT systems scale from localized networks to large-area infrastructures, the associated security risks have surged. This review addresses the key security challenges, protocols, and solutions being proposed to address these issues.

A major concern highlighted across the research is the lack of standardized protocols and architectures in IoT. Current IoT frameworks are vulnerable to various security threats due to their open architectures and weak security protocols. Studies, including those by Hamed Taherdoost et al. (2023) and Eisha Akansha et al. (2022), stress the need for stronger authentication and data protection mechanisms. Similarly, Vikas Hassija (2019) pointed out that the lack of standardization and system limitations exacerbates IoT security vulnerabilities, especially in wide-area networks where the exposure to cyber threats increases.

Moreover, IoT security requirements differ from traditional IT systems due to the diversity of IoT devices and the various layers they operate within, such as Perception, Network, and Application. Researchers like Shashi Rekha (2021) and Jean Pierre Nzabahimana (2018) have noted the prevalence of IoT-specific threats, including node capture, spoofing, and DDoS attacks, underscoring the need for security solutions that are tailored to IoT's unique characteristics.

Various studies, including those by Priyanka et al. (2019), have introduced multi-stage security models leveraging advanced encryption techniques like ECC and FHE. However, these models often face challenges such as increased computational overhead, which limits their effectiveness for resource-constrained IoT devices. Hongsong Chen (2019) proposed scalable architectures for low-energy IoT devices, but storage and energy demands remain significant hurdles.

Privacy is another critical concern. Researchers like Jyoti Neeli (2021) and Aldowah et al. (2019) emphasize the need for stronger intrusion detection systems and privacy-preserving methods in IoT systems. Balancing data security with maintaining the functionality of IoT systems is crucial for their continued growth.

In summary, securing IoT systems requires a comprehensive, multi-layered approach that incorporates solutions throughout the architecture. Future research must focus on creating scalable, efficient, and standardized security protocols capable of addressing multiple threat vectors while preserving the operational integrity of IoT devices. As IoT networks expand, ensuring data integrity, device security, and network defense will be vital. While recent studies have laid a strong foundation, further work is needed, especially in developing adaptable standards for the evolving IoT ecosystem.

The Internet of Things (IoT) encompasses a network of interconnected devices and objects, playing a significant role in automation and decision-making processes across various sectors. However, without appropriate security measures,

the benefits of this advanced technology may be diminished. This paper examines the impact of **Location Spoofing** and **Identity Spoofing** attacks on network performance. Through simulations in the Cooja simulator, it was observed that these attacks degrade network performance in several ways, such as increasing **power consumption**, reducing **throughput,** and introducing **delays**. Consequently, the overall lifespan of the IoT network is shortened.

Additionally, **ambiguous device identification** becomes a critical issue when **Location Spoofing** attacks are not properly addressed, further emphasizing the need for early detection and elimination of such threats during communication. As a future research direction, solutions could be developed to address both **Location Spoofing** and **Identity Spoofing** attacks by designing a **context-aware multi-attribute authentication methodology**. Moreover, enhancing the features of the **RPL protocol** to identify suspicious **IP-MAC address binding entries** and removing these records from the **Neighbour Cache (NC)** could provide additional protection against **Identity Spoofing** attacks.

REFRENCES

1. Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics 2023, 12, 1901. https://doi.org/10.3390/electronics12081901
2. Eisha, Akanksha., Abhishek, Javali., Jyoti. (2022). A review on Secutity in Internet of Things. 883-887. doi: 10.1109/AIC55036.2022.9848853
3. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
4. Rekha, Shashi & Lingala, Thirupathi & Renikunta, Srikanth & Gangula, Rekha. (2021). Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings. 10.1016/j.matpr.2021.07.295.
5. Jyoti Neeli, Shamshekhar Patil "Insight to security paradigm , research trend & statistics in internet of things(IoT)" Global Transitions Proceedings, Volume 2, Issue 1, 2021, Pages 84-90, https://doi.org/10.1016/j.gltp.2021.01.012.
6. Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021). https://doi.org/10.1007/s42452-021-04156-9
7. Wei Emma Zhang, Quan Z. Sheng et al. "The 10 Research Topics in the Internet of Things" published in 2nd IEEE International conference on RTEICT, 2020
8. Amit Kumar Tyagi and Ajith Abraham "Internet of Things: Future Challenging Issues and Possible Research Directions" published in International Journal of Computer Information Systems and Industrial Management Applications, Vol. 12, pp. 113-124, 2020.
9. H. Shin, H. K. Lee, H. Cha, S. W. Heo and H. Kim, "IoT Security Issues and Light Weight Block Cipher," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019, pp. 381-384, doi: 10.1109/ICAIIC.2019.8669029.
10. Hanan Aldowah, Irfan Kumar et al. "Security in Internet of Things: Issues, Challenges and Solutions" published at Springer Nature, 2019, pp. 396-405, DOI: 10.1007/978-3-319-99007-1_38.
11. Urla, Priyanka Anurag, et al. "A novel approach for security of data in IoT environment." Computing and Network Sustainability: Proceedings of IRSCNS 2018. Springer Singapore, 2019.
12. Jean Pierre Nzabahimana "Analysis of Security and Privacy Challenges in Internet of Things" presented at IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018
13. J. Voas, B. Agresti and P. A. Laplante, "A Closer Look at IoT 's Things," in IT Professional, vol. 20, no. 3, pp. 11-14, May./Jun. 2018, doi: 10.1109/MITP.2018.032501741. keywords: {Communication channels;Internet of Things;NIST;Computer security;internet of things;IoT;things;sensors;IoT devices;NIST;things and IoT;security;NoT;network of things;SP 800–183;NIST SP 800–183;IT Trends},
14. B V, Santhosh Krishna & Thangavel, Gnanasekaran. (2017). A systematic study of security issues in Internet-of-Things (IoT). 107-111. 10.1109/I-SMAC.2017.8058318.
15. Alizai, Z. A., Tareen, N. F., & Jadoon, I. (2018). Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. 2018 International Conference on Applied and Engineering Mathematics (ICAEM). doi:10.1109/ICAEM.2018.8536261
16. Alotaibi, M. (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN. IEEE Access: Practical Innovations, Open Solutions, 6, 70072–70087. doi:10.1109/ACCESS.2018.2880225
17. Aman, M. N., Basheer, M. H., & Sikdar, B. (2019). Two-Factor Authentication for IoT With Location Information. IEEE Internet of Things Journal, 6(2), 3335–3351. doi:10.1109/JIOT.2018.2882610
18. Chatterjee, B., Das, D., Maity, S., & Sen, S. (2019). RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning. IEEE Internet of Things Journal, 6(1), 388–398. doi:10.1109/ JIOT.2018.2849324
19. Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). doi:10.1109/I-SMAC.2017.8058363
20. Gope, P., & Sikdar, B. (2019). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. IEEE Internet of Things Journal, 6(1), 580–589. doi:10.1109/JIOT.2018.2846299
21. Loske, M., Rothe, L., & Gertler, D. G. (2019). Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). doi:10.1109/WFIoT.2019.8767327.
22. Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. doi:10.1016/j.comnet.2018.11.025
23. Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, L., Lun, L. S., Annuar Juma'at, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. IEEE Access: Practical Innovations, Open Solutions, 7, 151054–151089. doi:10.1109/ACCESS.2019.2947723
24. Naveed Aman, M., Taneja, S., Sikdar, B., Chua, K. C., & Alioto, M. (2019). Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff. IEEE Internet of Things Journal, 6(2), 2843–2859. doi:10.1109/JIOT.2018.2875472
25. Voas, J., Agresti, B., & Laplante, P. A. (2018). A Closer Look at IoT 's Things. IT Professional, 20(3), 11–14. doi:10.1109/MITP.2018.032501741
26. Wang, N., Jiang, T., Lv, S., & Xiao, L. (2017). Physical-Layer Authentication Based on Extreme Learning Machine. IEEE Communications Letters, 21(7), 1557–1560. doi:10.1109/LCOMM.2017.2690437
27. Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M.

(2018). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. IEEE Internet of Things Journal, 5(1), 269–282. doi:10.1109/ JIOT.2017.2780232

28. Zhao, Y., Li, S., & Jiang, L. (2018). Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment. Security and Communication Networks, 2018, 1–13. doi:10.1155/2018/9178941
29. Zhong, C. L., Zhu, Z., & Huang, R. G. (2017). Study on the IOT Architecture and Access Technology. 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES). doi:10.1109/ DCABES.2017.32
30. Cetintav and M. Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols From the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," in IEEE Access, vol. 13, pp. 37703-37723, 2025, doi: 10.1109/ACCESS.2025.3546147.
31. A. Sharma, R. Suganya, P. B. Krishna, R. Raj and R. Kumar Murugesan, "Network Efficient Hierarchical Authentication Algorithm for Secure Communication in IoT and IoE," in IEEE Access, vol. 12, pp. 195926-195942, 2024, doi: 10.1109/ ACCESS.2024.3516886.
32. Zhao, J.; Hu, H.; Huang, F.; Guo, Y.; Liao, L. Authentication Technology in Internet of Things and Privacy Security Issues in Typical Application Scenarios. Electronics 2023, 12, 1812. https://doi.org/10.3390/electronics12081812